Enterprise ITMC AD Team Recommendation

The purpose of this document is to summarize the recommendation of the Enterprise ITMC Active Directory (AD) Technical Team concerning the future deployment of AD.

The Enterprise AD Technical Team met numerous times between from July through the end of December 2011. The objective/goal of this team was to provide ITMC with an AD Configuration recommendation that the team thinks will best meet the State's business needs in the future.

The team was tasked with bringing forward a recommendation that would:

- Reduce the problems/costs associated with the current configuration while ensuring the appropriate and mandated security concerns are being addressed. The problems that will be addressed are defined in the Pain Points section of the May 13, 2011 Active Directory and Identify Findings.

- Ensuring the administrative functionality requirements associated with meeting state and federal auditors' requirements regarding who has administrative rights will be a key component of this recommendation.

- Ensure that security/administrative requirements that vary across agencies will be met.

- Where possible, facilitate joining Windows machines to Active Directory that are not currently joined due to security, privacy, and management concerns.

The team was sponsored by Stuart Fuller (SITSD) and consisted of Hunter Coleman (SITSD) Jerry Marks (DPHHS), Peder Cannon (DOR), Robert Cash (MDT), Josh Gillespie (LEG), Bryon Molyneaux (OPI), Rick Peaslee (DLI), and James Thomas (DOJ). The team activities were coordinated by Jim Sheehy (DOA – SITSD).

The team's activities consisted of:

1. Reviewing the State of Montana Active Directory and Identify Assessment Findings report that was submitted by Microsoft in May 2011 to ensure that the report identified all of the pain points that should be considered when creating business requirements.

2. Reviewing the options provided in the Microsoft documents. This review resulted in the team adding a fifth option. The fifth option consists of adding distributed identify Management software to the current hybrid administration model. It important to note the DPHHS is already in the process of setting up this environment using Microsoft Forefront Identify Management (FIM) and for the CHIMES2 project IBM's Tivoli Identity Manager.

3. Identifying Business Requirements associated with AD and Identity Management Processing. The team consistently struggled in this area, with the observation that the IT technical staff may not be the best group to identify and articulate agencies' business program requirements.

4. Evaluating the options using the Business Requirements to determine the options that should be brought forward to ITMC. Due to the challenges mentioned above, the resulting evaluations reduced to agency participants identifying the Option that they felt best suited their agency, along with general pro/con statements about all of the Options.

5. Making the recommendation to ITMC.

A variety of documents that include the team's Project Charter, Business Requirements, and agency evaluation are available on the Team's SharePoint site.
http://ent.sharepoint.mt.gov/sites/iatt/default.aspx

Two current issues in Active Directory design were addressed by the team in regards to OPI and DLI. OPI has a requirement for multiple school district employees to access applications being built by OPI development staff and contractors in a secure manner. DLI needs to manage multiple public access kiosk machines that are utilized by DLI Work Force Services Division.

The recommendations for DLI and OPI are:

1. Have OPI create a separate AD environment for the sole purpose of allowing School District employees to access OPI-managed applications. OPI either currently has, or must obtain, an exception to the E-Pass standard for storing identities used by the public to access state-provided services. OPI will still use the Enterprise AD environment to allow for any activity associated with state processing needs such as OPI employee user ID's and managing state owed devices. There won't be any connectivity (e.g. "Windows trust relationships") between the school district AD and the state Enterprise AD environments. Because OPI has a separate educational discount agreement with Microsoft, licensing for the school district users is handled by OPI. Establishing a separate AD forest for the school district employees will also allow OPI to remove a number of those School District users who currently have State AD user accounts from the enterprise AD forest.

2. Recommend that DLI explore the concept of joining the kiosk machines to the DMZ AD forest or establish a separate forest for management of the kiosk machines. This approach should be used by other agencies if they become responsible for devices that are used by the general public in the future. Using the DMZ AD forest reduces the duplication in infrastructure that would occur if multiple public kiosk AD forests were established by the State.

We estimate that the minimum annual costs for an agency running an Active Directory instance to be approximately $91,000 broken out as follows:

-staff time: one FTE, plus benefits: $85,000
-hardware/software/environmental/etc for 2 servers: $6,000

Note that the above figures do not include costs for additional domain controllers, server/service monitoring, auditing software or the staff time to manage monitoring and auditing. We estimate that the additional minimum annual costs for an agency running an Identity Management solution to be comparable to the costs required for running an Active Directory instance. Depending on the specific IdM solution and its licensing model, along with the degree of staff time necessary to customize the configuration, costs could significantly increase.

The next part of the recommendation consists of moving forward with **establishing Active Directory as the authentication and authorization directory of choice for the State. With this choice in directory services there is a recommendation of establishing trust relationships between the current AD environments and moving forward with the procurement of Identity Management software.** This recommendation comes with the following significant challenges that will require a considerable amount of effort and research to ensure we can move forward with this recommendation:

- The use of trust relationships will need to be reviewed and researched in depth to make sure everyone is aware of the risks associated with using trusts and how these risks can be mitigated. There are security concerns from both DOJ and DPHHS in regards to protecting of HIPPA and CJIN data.

- All agencies will need to support the procurement of Identity Management Software. The funding for this procurement may need to be part of this year's Executive Planning Process (EPP) which will be completed by the end of March 2012.

- The team would prefer to use an Identity Management solution with the same flexibility they have with the current AD environment. That being they would prefer to be responsible for their own Identity Management store.

- Option #5 presented by DPHHS was the choice of a majority of the team. This option basically allows for the use of agency Active Directory forests for users and resources where appropriate. Use of trust relationships and agency-run identity management solutions would provide for user authentication and, where appropriate, authorization.

- SITSD's position is that Option 4, which uses a single Identity management solution and trust relationships, is the preferred option. It is SITSD's opinion that multiple ID management solutions would increase both the complexity and the cost of managing user and resource identities. In order to provide for universal access to enterprise applications that use LDAP for authentication (SABHRS, FileNet) there needs to be a single LDAP directory that provides authentication and in the case of FileNet, group membership lookups. Any identity management solution or solutions will need to provide that functionality.